강 의 계 획 서

학습과정명	구분	교재명	저자명	출판사	출판연도	비고
인터넷보안	주교재	정보보안개론(4판)	양대일	한빛아카데미	2024	

학습목표	인터넷을 이용한 전자 상거래등 인터넷 보안과 관련해 실제 생활에 적용하고 있는 인터넷 보안의 기본 개념과 원리를 이해시키고 이를 바탕으로 인터넷보안 분야의 기본 소양을 습득하기 위해 각종 암호 기술, 보안 프로토콜, 공개키 기반구조, 전자 화폐 기술등의 내용을 학습하도록 한다. 이에 따라 본 교과목의 목표는 암호의 개요 및 암호 알고리즘, 암호 프로토콜의 개념을 습득하게 하고 이를 활용한 인터넷 보안 서비스인 공개키 기반구조, 전자우편, 전자화폐, 악성코드, 침입탐지 시스템 등에 대해서 학습함으로써 실생활에서의 인터넷 보안을 이해하고, 사용할 수 있도록 학습하도록 한다.

학점	3학점	**정원**	40명
수업 기간 (※학사일정 참고)	1. 1학기: 3월 ~ 6월 (15주) 2. 여름 계절학기: 7월 ~ 8월 (8주) 3. 2학기: 9월 ~ 12월 (15주) 4. 겨울 계절학기: 1월 ~ 2월 (8주)	**주당 시수 / 총 시수**	3시간 / 45시간
교·강사명	김은환 등 5명	**수강료**	420,000원

성적평가 방법(평가요소)

중간고사	기말고사	과제물	출결	기타	합계	비고
30%	30%	10%	20%	10%	100%	기타- 수시시험

학습과정명	인터넷보안

■ 주차별 수업(강의 • 실험 • 실습 등) 내용

주별	차시	주차별 수업(강의•실험•실습 등) 내용	과제 및 기타 참고사항
1	1 2 3	: 과목에 대한 전반적인 소개의 시간을 갖는다. 한 학기 동안 이루어질 강의 내용에 대한 이해를 시킨다. 인터넷 보안을 학습하기 위한 기본 지식을 테스트 한다. 간이 시험 형식을 통해 사전에 작성한 문제를 활용하여 시험을 실시한다. 정보 보안의 세계에 대한 대략적인 내용을 설명한다. 특히, 해킹 보안의 역사와 보안의 3대 요소를 설명한다. (주교재 -> 1장 : 정보 보안의 세계)	
2	1 2	인터넷 보안 분야 중 시스템 보안에 대한 개념을 설명한다. 특히, 시스템 보안에서 다루어야 계정관리, 패스워드관리 및 세션관리 대해서 간략하게 학습한다. 운영체제에서 사용하는 계정과 패스워드 관리에 대해서 학습한다. 또한, 데이터베이스 및 기타 응용 프로그램에서의 계정관리와 패스워드 작성	

		요령 등에 대해서 설명한다. 인터넷이 연결된 후에 주의해야 할 세션관리와 접속된 후에 접근할 수 있는 운영체제, 데이터베이스 및 네트워크 장비의 접근 제어에 대해서 학습한다. (주교재 -> 2장 : 시스템 보안) 강의방법: 강의, 질의응답, 토론(일상적인 생활에서 LINUX시스템 및 각종 웹사이트에서의 계정관리에 대해서 토론해 본다.)	
	3		
3	1	: 시스템 보안 중에서 권한 관리에 대해서 학습한다. 권한 관리는 운영체제, 데이터베이스에 대해서 접속하여 시스템을 사용할 수 있는 권한을 획득하고 사용할 수 있는 방법 등에 대해서 알아본다. 운영체제나 데이터베이스 및 기타 응용 프로그램등에 접속하여 자원을 사용할 때는 사용자나 사용 시간 및 접속 횟수등에 대한 기록에 대한 관리를 한다. 이를 로그 관리라 하며 이를 학습한다. 시스템은 일정 시간이 지나고 나면 취약점이 발생하게 된다. 이를 패치 관리를 통해 보완한다. 이처럼 시스템에서 발생하는 취약점을 분석하고 보완할 수 있는 방법에 대해서 학습한다. (주교재 -> 2장 : 시스템 보안) 강의방법: 강의, 질의응답, 토론(리눅스의 권한 설정 방법에 대해서 토론한다.)	
	2		
	3		
4	1	네트워크 보안을 이해하기 위해 OSI 7계층의 각각의 역할에 대해서 학습한다. 각각의 역할을 통해서 통신되는 원리를 이해한다. 서비스 거부(DoS) 공격에 대해서 학습한다. 특히, 서비스 거부 공격의 유형인 취약점 공격과 자원 고갈 공격형에 대해서 알아본다. 또한, 분산 서비스 거부(DDoS)도 학습한다. 네트워크 공격중에서 스니핑 공격에 대해서 알아본다. 스니핑 공격의 원리와 스위치 재밍 공격 및 SPAN 포트 태핑 공격에 대해서 학습한다. 또한, 스니퍼를 탐지하는 방법에 대해서도 알아본다. (주교재 -> 3장 : 네트워크 보안) 강의방법: 강의, 질의응답, 토론, 발표 (발표 : 네트워크의 기본 계층인 OSI 7계층에 대해서 조사하여 학생들이 발표한다.)	
	2		
	3		
5	1	스푸핑 공격에 대한 이론에 대해서 알아본다. 스푸핑 공격의 유형인 ARP 스푸핑 공격, IP 스푸핑 공격, ICMP 리다이렉트 공격, DNS 스푸핑 공격등에 대해서 자세하게 학습한다. 네트워크 보안중에서 세션 하이재킹 공격에 대해서 학습한다. 세션이란 사용자와 컴퓨터간의 활성화된 상태이므로 이들 사이에 간섭하여 데이터를 탈취하는 방법이다. 다양하게 사용되어지는 무선 네트워크에 대한 공격과 이를 방지하는 방법에 대해서 학습한다. AP보안, 무선 랜 통신 암호와 방법, EAP암호화 방법에 대해서도 알아본다. (주교재 -> 3장 : 네트워크 보안)	※수시시험 (5점) - 쪽지시험 실시
	2		
	3		

		강의방법: 강의, 질의응답, 토론(ARP 스푸핑에 대해서 조사하고 토론한다.)	
6	1 2 3	웹 보안에 대해서 학습하기 위해서 웹에 대한 이해를 한다. 특히, 웹 프로토콜인 HTTP프로토콜에 대해서 알아본다. 웹 보안을 이해하기 위해 웹에서 제공하는 서비스들에 대해서 상세하게 이해할 필요가 있다. 웹 서비스에는 HTML, SSS, CSS, SSL/TLS등이 있으며 이를 세부적으로 학습한다. 웹 해킹 방법에 대해서 알아본다. 웹 해킹 방법은 웹 취약점 스캐너를 통해 정보를 수집하고 웹 프록시를 통한 취약점을 분석한다. 또한, 구글 해킹을 통해서도 정보수집이 가능하다. (주교재 -> 4장 : 웹 보안) 강의방법: 강의, 질의응답, 토론(HTTP 프로토콜의 동작 원리에 대해 학생들의 조사 및 토론을 한다.)	
7	1 2 3	: 웹의 상당히 다양한 취약점을 지니고 있으며 이를 세부적으로 학습한다. 명령 삽입 취약점, XSS 취약점, 취약한 인증 및 세션 관리, 직접 객체 참조, CSRF 취약점등에 대해서 학습한다. 웹의 취약점에 대해서 학습한다. 보안 설정 취약점, 취약한 정보 저장 방식, URL 접근 제한 실패, 인증시 비 암호화 채널 사용, 부적절한 오류 처리에 대한 취약점을 학습한다. 웹에서 발견된 취약점을 보완하는 방법을 학습한다. 이를 위해서 특수 문자 필터링 방법, 서버 측 통제 적용 방법, 지속적인 세션 관리 방법에 대해서 알아본다. (주교재 -> 4장 : 웹 보안) 강의방법: 강의, 질의응답, 토론(XSS 취약점에 대한 학생들 조사후 토론한다.)	
8	1 2 3	중간고사	
9	1 2 3	: 코드보안에 대해서 알아보기 위해 시스템과 프로그램에 대해 이해한다. 특히, 시스템 메모리의 구조와 프로그램 실행 구조에 대해서 학습한다. 버퍼 오버플로우 공격에 대해서 자세하게 학습한다. 버퍼 오버플로우의 개념과 공격의 원리 및 공격에 대한 대응책에 대해서 알아본다. 포맷 스트링 공격에 대해서 자세하게 알아본다. 포맷 스트링의 개념 및 공격의 원리, 그리고 대응책에 대해서 학습한다. (주교재 -> 5장 : 코드 보안) 강의방법: 강의, 질의응답, 토론(포맷 스트링 공격에 대해 학생 조사 후 토론한다.)	
10	1	: 악성코드의 역사와 악성코드의 분류에 대해서 알아본다. 악	

		성코드는 바이러스와 웜으로 분류되며, 바이러스를 역사적으로 구분하여 학습한다. 웜에 대한 생성 원인과 웜의 분류인 MASS Mailer형 웜, 시스템 공격형 웜등에 대해서 원인과 대응책에 대해서 학습한다. 그 외의 여러 가지 악성코드에 대해서 알아본다. 특히, 백도어와 트로이 목마 및 인터넷 악성코드들에 대해 분석하고 악성코드 탐지 및 대응책에 대해서 학습한다. (주교재 -> 6장 : 악성 코드) 강의방법: 강의, 질의응답, 토론, 발표 (발표 : 시스템 보안, 네트워크 보안, 웹 보안, 코드 보안에 대해서 정리하여 학생이 조사하여 발표한다.)	
	2		
	3		
11	1	암호의 발전사를 통해서 암호화 과정을 이해하고 최초의 암호 시스템, 전치법 및 대체법등에 대해서 자세하게 학습한다. 암호화 방식의 대표적인 방식으로 대칭 암호화 방식에 대해서 학습한다. DES 알고리즘, 트리플 DES 알고리즘, AES 알고리즘에 대해서 알아본다. 비대칭 암호화 방식의 필요성에 대해서 알아보고, 대표적인 비대칭 암호화 방식인 DES알고리즘을 학습한다. 또한, 해쉬 알고리즘의 역할 및 종류에 대해서도 알아본다. (주교재 -> 7장 : 암호의 이해) 강의방법: 강의, 질의응답, 토론	
	2		
	3		
12	1	전자상거래에 대한 이해와 전자상거래의 보안 요건 및 공개키 기반 구조의 개념과 공인 인증서에 대해서 학습한다. 안전한 전자 상거래를 위해서 필수적인 사항인 전자서명과 전자봉투에 대한 개념 및 원리에 대해서 알아본다. 전자상거래를 위한 전자결재 시스템인 SET과 Cyber Cash, 스마트 카드에 대해서 알아본다. 또한, 내용을 안전하게 전달 할 수 있는 컨텐츠 보안인 스테가노그래피와 워터마크에 대해서 학습한다. (주교재 -> 8장 : 전자 상거래 보안) 강의방법: 강의, 질의응답, 토론, 과제설명	※과제 (10점) : 암호를 이용한 전자상거래의 동작원리에 대해서 정리하고, 전자상거래의 예시와 시스템보안에 대한 구체적인 예시를 조사하여 제출한다. (14주차 제출, 기간 내 미제출 시 감점)
	2		
	3		
13	1	접근하려는 개체의 신원을 확인하는 방법인 인증 방법에 대하여 알아본다. 또한 방화벽에 구조와 원리 및 주요 기능에 대해서도 학습한다. 침입탐지 시스템의 주요 기능 및 설치 위치와 그 역할에 대해서 알아본다. 또한, 침입 방지 시스템의 동작 원리 및 설치 위치에 대해서도 학습한다. VPN의 기능 및 역할에 대해서 자세하게 학습하고 기타 출입 통제 및 모니터링 장비에 대해서 알아본다. 그 외의 기타 보안 솔류션에 대해서 확인해 본다. (주교재 -> 9장 : 보안 시스템) 강의방법: 강의, 질의응답, 토론	※수시시험 (5점) - 쪽지시험 실시
	2		
	3		

14	1 2 3	침입 대응에 대한 이해를 한다. 침입대응에는 사전대응, 사고탐지, 제거 및 복구 후속 조치 및 보고의 순서로 침입 대응을 진행한다. 포렌식이란 무엇인지를 확인하고 증거에 대한 이해와 포렌식의 기본 원칙 및 포렌식 수행 절차와 사이버 수사 기구에 대해서 학습한다. 네트워크상에서 이루어지는 범죄에 대한 증거 수집 방법 및 절차와 시스템(PC)에서의 증거수집 방법에 대해서 알아본다. 또한 데이터 및 응용 프로그램에서의 증거 수집 방법도 확인해 본다. (주교재 -> 11장 : 침해 대응과 디지털 포렌식) 강의방법: 강의, 질의응답, 토론(사이버 수사대에 대한 학생 조사 후 토론 한다.)	
15	1 2 3	기말고사	

※ 강의계획서 주차별 내용은 교·강사에 따라 변동될 수 있습니다.